REMARKS

In response to the Office Action mailed December 30, 2004, Applicant respectfully requests reconsideration. By this amendment, claims 1, 6, 15 and 21 have been amended. Claims 33 and 34 are new. Accordingly, claims 1-4, 6-27 and 29-34 are pending in this application, of which claims 1, 15 and 21 are independent claims.

I. Brief Summary of Response

In a previous Response mailed on August 4, 2003, Applicant argued that there is no motivation to combine Ericson (U.S. Patent No. 6,061,753) and Yu (U.S. Patent No. 4,919,545). To advance prosecution, Applicant amended the claims (see the Amendment filed on November 8, 2004) to distinguish over the combination, rather than continue to argue it, even though Applicant believed the combination to be improper. However, Applicant has reconsidered the decision to amend the claims and herein reverts to pointing out that the combination of Ericson and Yu is improper.

Accordingly, Applicant has broadened the scope of the claims by removing the claim amendments made in the Amendment of November 8th. The claims as now presented are substantially as they appeared in the Response of August 4th. Applicant addresses below the "Response to Arguments" made in the Office Action mailed May 6, 2004, which stated that Applicant's arguments were not persuasive in showing a lack of motivation to combine Ericson and Yu.

II. Rejection Under 35 U.S.C. §103

In the Office Action, all of the claims (including independent claims 1, 15 and 21) are rejected under 35 U.S.C. 103(a) as purportedly being obvious over Ericson (U.S. Patent No. 6,061,753) in view of Yu (U.S. Patent No. 4,919,545) and Abadi et al. (U.S. Patent No. 5,315,657). This rejection is respectfully traversed.

A. There is No Motivation to Combine Ericson and Yu

There is no motivation for the reasons in the prior response dated August 4, 2003, which is incorporated herein by reference. In the Response to Arguments presented in the final Office Action mailed May 6, 2004, the Office Action asserts that Applicant's arguments were unpersuasive because "Ericson clearly concerned with security and prevention of unauthorized

access to the storage system by host devices over the network [see col.1 lines 62 to col.2 lines 3]." However, the portion of Ericson cited by the Examiner merely describes the privacy problem of conventional systems that results when the entire disk array is accessible by all of the host computers. That is, the information belonging to one host computer is visible and accessible by another because no *authorization* scheme is in place. This does not speak to the issue of trust and trusted environments. The question of whether an environment is trusted does not turn on whether a host will access information that is made available to it, but whether a host can be trusted with respect to its identity. That is, an untrusted environment is one, for example, where the devices connected to the network may be widely distributed and unknown, such that a request from a given host may not be trusted to genuinely be from that host rather than another attempting to spoof its identity to gain access to unauthorized information.

Ericson and Yu address entirely different "security" issues. Applicant's argument is not that Ericson is unconcerned with security, but rather that the security measures taught by Yu (i.e., authentication) are not relevant and have no bearing in the context of Ericson. It should be appreciated that *authorization* and *authentication* are two distinct security measures that address separate and distinct security issues. Ericson addresses the former, but has no need to address the latter. Thus, Applicant points out that one skilled in the art would not have been motivated to implement authentication techniques because such techniques are unnecessary and provide no security benefit in the environment of Ericson.

In particular, in the Ericson environment, an administrator sets up a local SCSI network with devices having access to a networked disk array. The administrator partitions access to the disk array by setting up a look-up table authorizing certain devices to access certain portions of the disk array, thus avoiding the privacy issues identified in col. 1, line 62 – col. 2, line 3. However, authentication of a device's represented identity is unnecessary because all the devices on the network are known and trusted not to spoof the identity of another device. As discussed in detail in Applicant's August 4th Response, the SCSI network is a local and contained network of devices wherein each of the devices is connected, configured and known by an administrator of the network. Not only are there no untrusted devices on the SCSI network, but the SCSI network itself prevents devices from spoofing their identity to gain access credentials of another device.

In Ericson, the networked data storage environment consists of the sharing of a disk array by a small number of known, local and contained devices. In this environment, authentication is not necessary and would serve only as a superfluous design addition. Nowhere does Ericson disclose an environment where untrusted devices have access to the data storage, nor does Ericson suggest that spoofing is, or would be, a problem. The authenticity issues addressed by Yu simply do not exist in the environment of Ericson since hosts attempting to fool the authorization scheme by spoofing their identity is not a problem, if even a possibility, in Ericson. The alleged modification would have no security benefit in the networked data storage environment of Ericson and, therefore, one skilled in the art would not have been motivated to make the modification. Therefore, it is respectfully asserted that the Office Action has failed to establish a *prima facie* case of obviousness and the rejection is therefore improper. Applicant respectfully requests that the rejection be withdrawn.

III. New Claims

Claims 33 and 34 have been added to incorporate at least some of the subject matter removed from independent claim 1. In particular, claim 33 recites acts of transferring an expected access key between the storage system and the at least one of the at least two devices, including a request access key in a subsequent request, and comparing the request access key and the expected access key for verification. Claim 34 recites the act of encrypting the expected access key and/or the request access key with encryption information transferred between the storage system and devices connected thereto. Both claims 33 and 34 depend from claim 1 and are patentable for at least the same reasons. No new matter has been added.

CONCLUSION

In view of the foregoing amendments and remarks, this application should now be in condition for allowance. A notice to this effect is respectfully requested. If the Examiner believes, after this amendment, that the application is not in condition for allowance, the Examiner is requested to call the Applicant's attorney at the telephone number listed below to discuss any outstanding issues relating to the allowability of the application.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicant hereby requests any necessary extension of time. If there is a fee occasioned by this response, including an extension fee, that is not covered by an enclosed check, please charge any deficiency to Deposit Account No. 23/2825.

Respectfully submitted,
Steven M. Blumenau et al., Applicant

By: _____

Richard F. Giunta, Reg. No. 36,149
Wolf, Greenfield & Sacks, P.C.
600 Atlantic Avenue
Boston, Massachusetts 02210-2211
Telephone: (617) 720-3500

Docket No.E0295.70066US00
Date: June 30, 2005
x06/30/05